OIPE
JUN 3 0 2005
PATENT & TRADEMARK

3/9

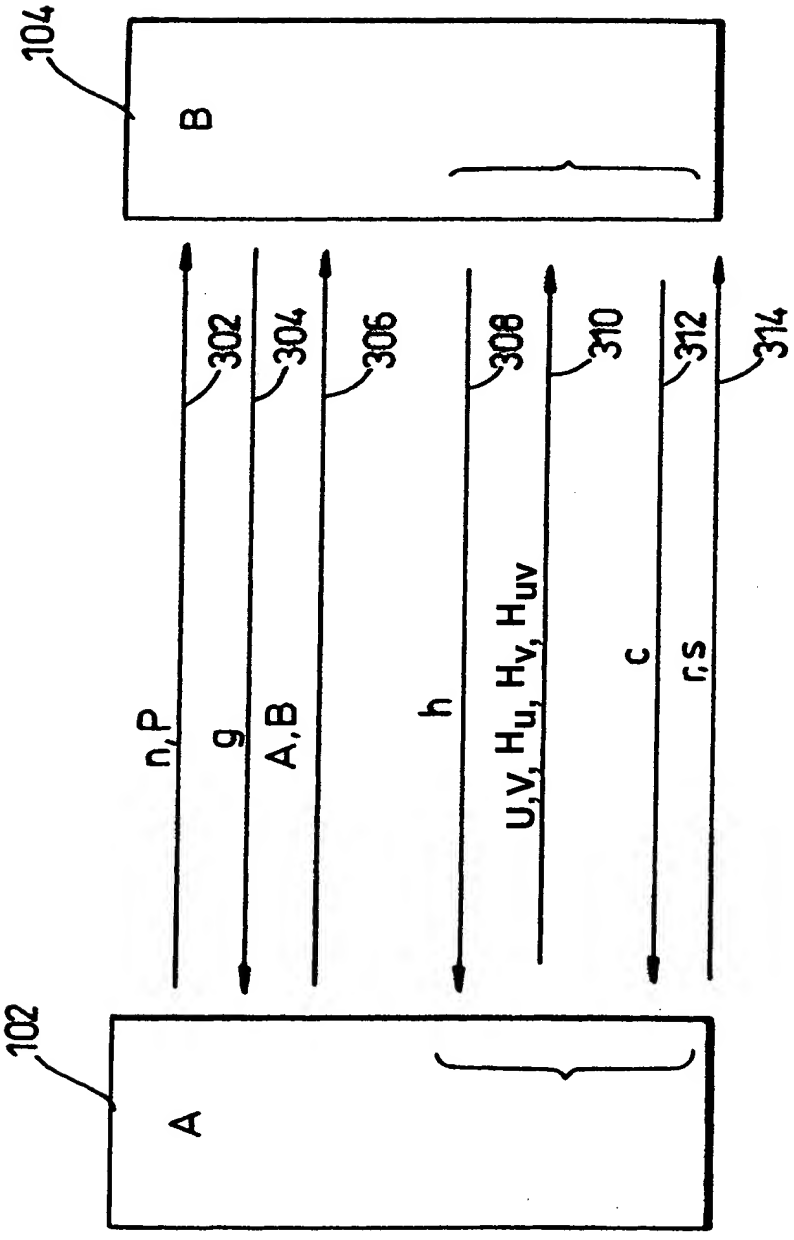

Fig. 3

5/9

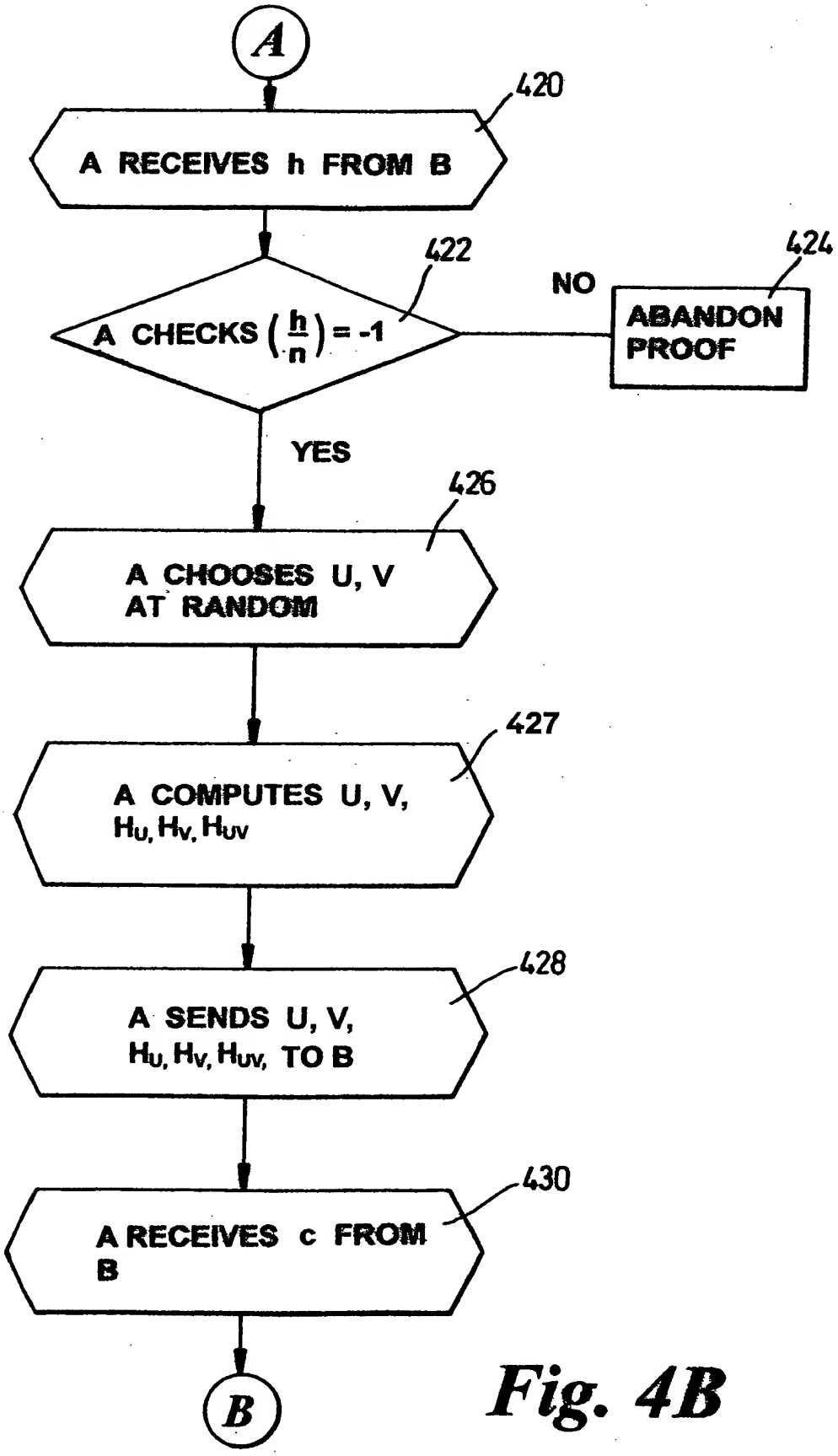
A
420
A RECEIVES h FROM B
422
A CHECKS $\left(\frac{h}{n}\right) = -1$
NO
424
ABANDON PROOF
YES
426
A CHOOSES U, V AT RANDOM
427
A COMPUTES U, V, H_U, H_V, H_{UV}
428
A SENDS U, V, H_U, H_V, H_{UV}, TO B
430
A RECEIVES c FROM B
B

Fig. 4B

7/9

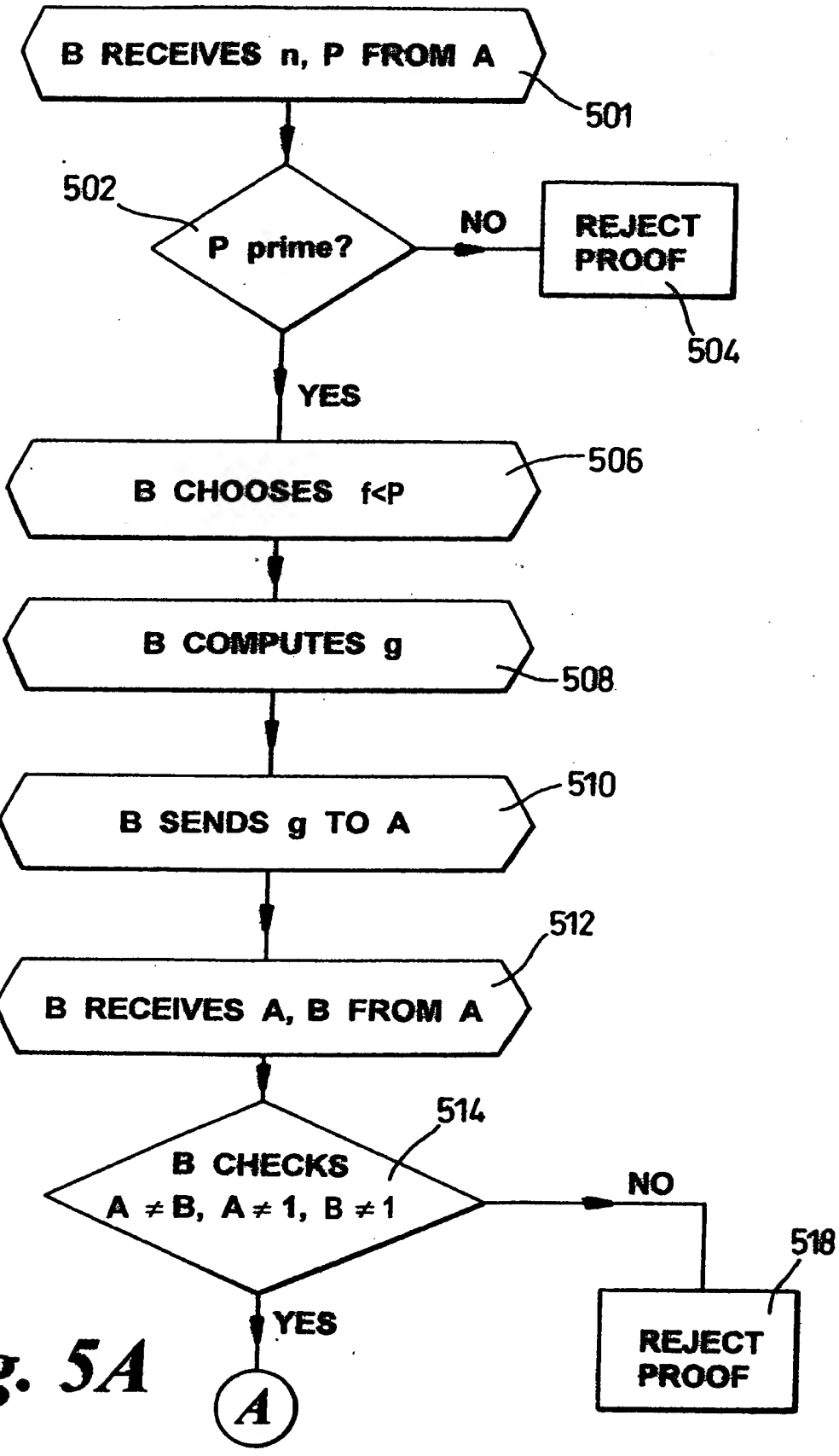
B RECEIVES n, P FROM A
501
502
P prime?
NO
REJECT PROOF
504
YES
B CHOOSES f<P
506
B COMPUTES g
508
B SENDS g TO A
510
B RECEIVES A, B FROM A
512
B CHECKS
A ≠ B, A ≠ 1, B ≠ 1
514
NO
518
REJECT PROOF
YES
A

Fig. 5A

9/9

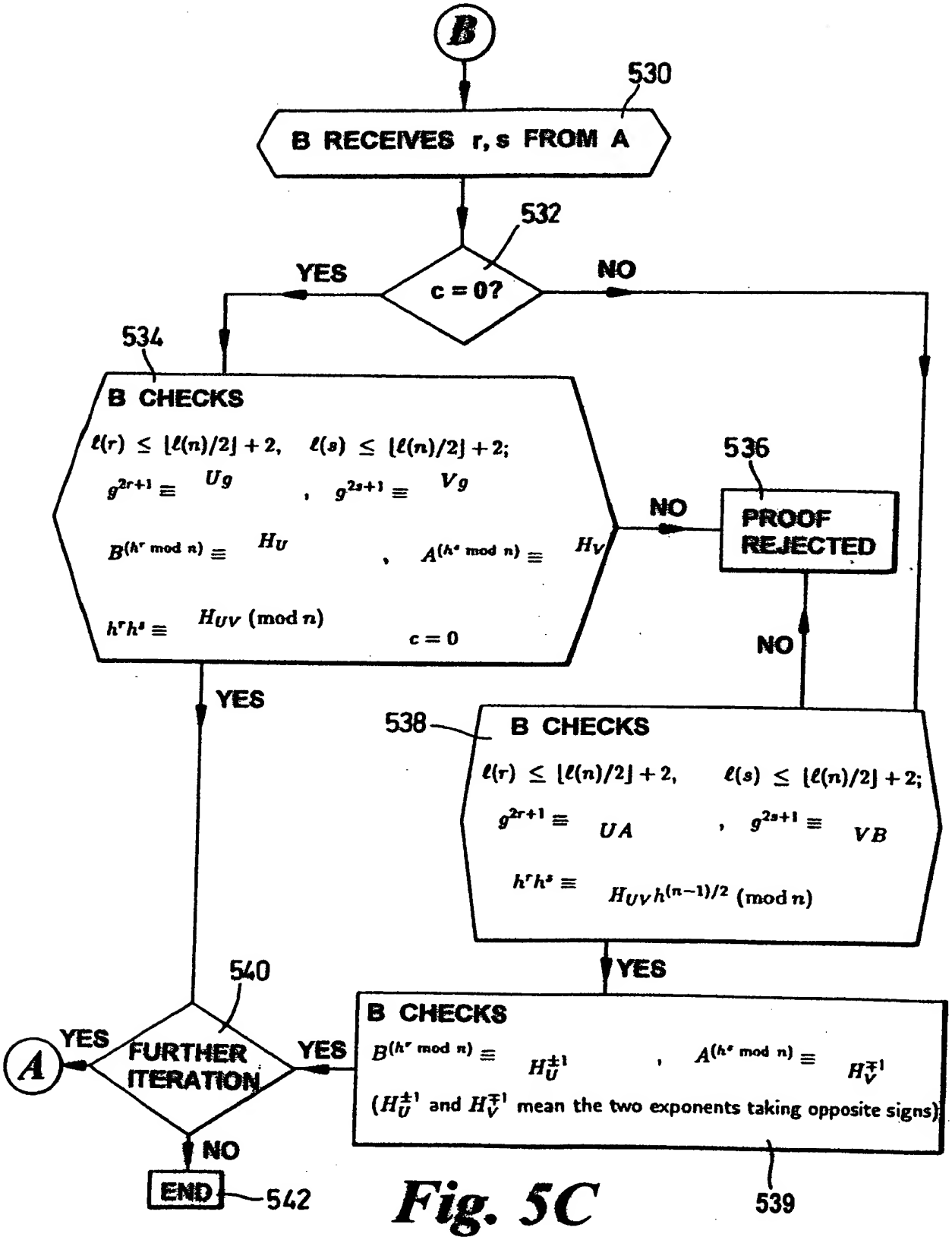
B
530
B RECEIVES r, s FROM A
532
c = 0?
YES
NO
534
B CHECKS
$\ell(r) \leq \lfloor \ell(n)/2 \rfloor + 2, \quad \ell(s) \leq \lfloor \ell(n)/2 \rfloor + 2;$
$g^{2r+1} \equiv Ug \quad , \quad g^{2s+1} \equiv Vg$
$B^{(h^r \bmod n)} \equiv H_U \quad , \quad A^{(h^s \bmod n)} \equiv H_V$
$h^r h^s \equiv H_{UV} \pmod n$
$c = 0$
536
NO
PROOF REJECTED
NO
YES
538
B CHECKS
$\ell(r) \leq \lfloor \ell(n)/2 \rfloor + 2, \quad \ell(s) \leq \lfloor \ell(n)/2 \rfloor + 2;$
$g^{2r+1} \equiv UA \quad , \quad g^{2s+1} \equiv VB$
$h^r h^s \equiv H_{UV} h^{(n-1)/2} \pmod n$
YES
540
A
YES
FURTHER ITERATION
YES
B CHECKS
$B^{(h^r \bmod n)} \equiv H_U^{\pm 1} \quad , \quad A^{(h^s \bmod n)} \equiv H_V^{\mp 1}$
($H_U^{\pm 1}$ and $H_V^{\mp 1}$ mean the two exponents taking opposite signs)
NO
END
542
539

Fig. 5C